

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Three Smartphones: Motorola, XT1921-3, IMEI:

354159100689047; LG, LM-X220MA, IMEI:

352533-10-124096-2; ZTE, Z836BL, IMEI: 8624470326584

Case No.

19-1061M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, incorporated here.

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

See attachment B, incorporated here.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

21 U.S.C. Sect. 841(a)(1);

21 U.S.C. Sect. 846.

Offense Description

Distribution of a controlled substance; and
 conspiracy to distribute a controlled substance..

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Robert Wise, Special Agent, ATF

Printed name and title

Sworn to before me and signed in my presence.

Date:

6/18/19

Judge's signature

City and state: Philadelphia, PA.

U.S. Magistrate Judge Elizabeth T. Hey

Printed name and title

19-1061M

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Robert Wise, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—three electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) and have been since 2015. I am currently assigned to ATF Philadelphia Group VII, which is a Firearms Enforcement Group whose primary responsibilities include investigating individuals or groups who commit violations of federal firearms and narcotics laws in Philadelphia, Pennsylvania. As a result of my training and experience, and that of other investigators, I am familiar with and have conducted investigations involving violations of Federal narcotics laws, and I am familiar with Federal search warrants and seizing evidence in accordance with the probable cause set forth in the affidavits. I have attended training encompassing and am familiar with the use of cellular phones and electronic communication to facilitate criminal activities.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched consists of three electronic devices (collectively referred to as “the Devices”), as follows:

- a. Motorola, Model XT1921-3 smartphone, with IMEI: 354159100689047, hereinafter referred to as “Device A;”
- b. LG, Model LM-X220MA smartphone, with IMEI: 352533-10-124096-2, bearing telephone number (267) 438-5835, hereinafter referred to as “Device B;” and
- c. ZTE, Model Z836BL smartphone, with IMEI: 862447032658403, hereinafter referred to as “Device C.”

5. The Devices are currently located at the ATF offices located at the United States Customs House, 200 Chestnut Street, Philadelphia, Pennsylvania.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. The United States, including the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) and the Drug Enforcement Administration (“DEA”), in conjunction with the Philadelphia Police Department (“PPD”), is conducting a criminal investigation of several individuals known and unknown, including John PHILLIPS, for distribution of a controlled substance in violation of 21 U.S.C. § 841 and conspiracy to distribute a controlled substance in violation of 21 U.S.C. § 846. The investigation has revealed that PHILLIPS has distributed and conspired to distribute methamphetamine in Philadelphia, PA, and that he utilizes cellular telephones in furtherance of this distribution.

Controlled Methamphetamine Purchases from SELLER-1

8. On March 8, 2019, and on March 15, 2019, an ATF Special Agent acting in an undercover capacity (hereinafter referred to as “UC-1”) and an ATF Confidential Informant¹ (hereinafter referred to as “CI-1”) working together conducted controlled purchases² of methamphetamine³ from a known individual (hereinafter referred to as “SELLER-1”) in a parking lot in Philadelphia, PA. During the controlled purchase on March 8, 2019, SELLER-1 provided his telephone number (hereinafter referred to as “SELLER-1 PHONE”) to CI-1 in order to arrange future narcotics transactions.

**SELLER-1 Phone Contacts with DEVICE B
during March 27, 2019 Controlled Purchase**

9. On March 24, 2019, CI-1 contacted SELLER-1 via the SELLER-1 PHONE number and arranged to purchase methamphetamine from SELLER-1 on March 27, 2019. On March 25, 2019, the Honorable Timothy Rice, United States Magistrate Judge for the Eastern District of Pennsylvania, signed a court order authorizing the installation of a pen register and trap and trace device (hereinafter referred to as “the SELLER-1 pen register”) on the SELLER-1 PHONE, allowing for the real-time recording, decoding, and/or capturing of dialing, routing, addressing, and signaling information associated with each communication to or from the

¹ CI-1 is a registered ATF Confidential Informant. CI-1 has participated in multiple prior ATF investigations, including conducting numerous successful controlled purchases of firearms and bulk quantities of narcotics that have resulted in both federal and state prosecutions. CI-1 is not exposed to federal or state prosecution at this time.

² A “controlled purchase” is when investigators use an undercover officer and/or a confidential informant to purchase evidence, such as narcotics, from subjects of an investigation. Audio/video electronic surveillance equipment is used to record the transaction and physical surveillance is conducted by investigators.

³ Samples of all of the methamphetamine referenced in this affidavit has been field tested by the Drug Enforcement Administration, and all these field tests have been positive for methamphetamine. Analysis by DEA regarding the purity of this methamphetamine is currently pending.

SELLER-1 PHONE by ATF. ATF began to receive this information from the SELLER-1 pen register on March 26, 2019.

10. On March 27, 2019 UC-1 and CI-1 met with SELLER-1 in the aforementioned parking lot in Philadelphia, PA in order to purchase methamphetamine. Through prior telephone contacts with SELLER-1, UC-1 and CI-1 understood that SELLER-1 would not have the methamphetamine with him when they met, but that it would be brought by another individual who would arrive later. SELLER-1 waited with UC-1 and CI-1 in this parking lot for approximately 45 minutes. UC-1 and CI-1 understood that they were waiting with SELLER-1 for the supplier of the methamphetamine to arrive at the parking lot. While waiting with SELLER-1, UC-1 and CI-1 observed SELLER-1 answer an incoming call on his cellular phone. During this call, UC-1 and CI-1 overheard SELLER-1 state to someone on the other end of this call that he saw them and that he would be right over. During this call, UC-1 observed SELLER-1 look toward an area of the parking lot where, a short time later, ATF personnel determined an Audi SUV bearing Pennsylvania tag KXX-9805 to be parked. Immediately after this call, SELLER-1 informed UC-1 and CI-1 that "it" was here, an apparent reference to the methamphetamine, and that he would be right back. UC-1 then paid SELLER-1 with government funds. ATF personnel observed as SELLER-1 walked a short distance to the passenger side of the Audi SUV, which SELLER-1 appeared to enter. Several minutes later, ATF personnel observed SELLER-1 walk from the passenger side of the Audi back to where UC-1 and CI-1 were waiting. Once there SELLER-1 provided CI-1 with a bag containing approximately 222 grams of methamphetamine. ATF personnel observed the Audi drive away mere moments after SELLER-1 appeared to exit it. Through analysis of the SELLER-1 pen register, ATF determined 267-438-5835 (hereinafter

referred to as "DEVICE B") to be the telephone number that SELLER-1 had been in contact with in order to coordinate the delivery of this methamphetamine.

John PHILLIPS Links to DEVICE B

11. I have consulted with an agent of the Pennsylvania Board of Probation and Parole (PBPP), with whom PHILLIPS is currently on active supervision as part of a term of parole. As part of the terms of his supervision by PBPP, PHILLIPS is required to provide PBPP with a current telephone number. PBPP informed me that PHILLIP's telephone number is 267-438-5835, the telephone number for DEVICE B⁴.

**John PHILLIPS and DEVICE B Continued Involvement
in Distribution of Methamphetamine**

12. On April 12, 2019 UC-1 and CI-1 again met with SELLER-1 in the aforementioned parking lot in Philadelphia, PA in order to purchase additional methamphetamine. During this meeting, SELLER-1 told UC-1 and CI-1 that the source of the methamphetamine had received the methamphetamine the night before. During this meeting, UC-1 and CI-1 observed SELLER-1 speak to someone on his cellular phone. The SELLER-1 pen register shows that at approximately the time that UC-1 and CI-1 observed this call, DEVICE B was calling SELLER-1. UC-1 was able to overhear a portion of this conversation. UC-1 heard SELLER-1 ask the individual on the other end of the call whether to meet where

⁴ DEA has obtained subscriber information for the DEVICE B telephone number, which lists the subscriber's name as "Shreef Austin" and the subscriber's address as 1726 N 16th Street, Philadelphia, PA 19121. I have queried Pennsylvania Department of Transportation records, and have been unable to locate any record of a Pennsylvania driver's license or identification card issued in either the name "Shreef Austin" or "Austin Shreef". In my training and experience, I know it to be common for individuals engaged in drug trafficking, such as PHILLIPS, to list their telephones in a third person's name or under a fictitious name in in order to mask their direct linkage to telephones utilized in furtherance of drug trafficking activities. With regard to the address listed in the subscriber information, I have reviewed Bensalem Police Department paperwork concerning an arrest of John PHILLIPS on October 3, 2016 in Bensalem, PA. In this paperwork, PHILLIPS' home address is listed as 1726 N 16th St, Philadelphia, PA 19121, corresponding to the subscriber's address listed for DEVICE B.

they were at last time, then agree to what the individual on the other end of the line stated. SELLER-1 then instructed UC-1 and CI-1 to follow him. UC-1 and CI-1 then followed SELLER-1 as he drove to the 2700 block of W Cambria Street, where SELLER-1 and UC-1, who was accompanied by CI-1, parked their vehicles and waited. A short time after SELLER-1, UC-1, and CI-1 arrived on the 2700 block of W Cambria Street, investigators observed John PHILLIPS exit the front door of a residence at 2824 N Marston Street and walk directly to the 2700 block of W Cambria Street while carrying a black plastic bag in his hand. Investigators observed PHILLIPS meet briefly with SELLER-1. SELLER-1 then immediately walked to UC-1 and CI-1 and provided them the aforementioned black plastic bag, which was found to contain approximately 228 grams of methamphetamine. Investigators observed as PHILLIPS immediately walked back to and re-entered the front door of 2824 N Marston Street. A review of PHILLIPS' Pennsylvania driver's license information reveals that PHILLIPS' currently lists his address as 2824 N Marston Street, Philadelphia, PA.

13. On April 29, 2019 CI-1 arranged via telephone to meet with SELLER-1 on April 30, 2019 to purchase additional methamphetamine. Later on April 29, the SELLER-1 pen register shows that SELLER-1 contacted DEVICE B via text message, which was then followed by multiple text messages and voice calls between SELLER-1 and DEVICE B on April 29. On April 30, SELLER-1 contacted CI-1 via telephone and arranged to meet with CI-1 in a location where they had not previously met in order to conduct the methamphetamine transaction. SELLER-1 and CI-1 engaged in a series of back-and-forth telephone contacts as SELLER-1 directed CI-1 and UC-1 to the meeting location. The SELLER-1 pen register shows that prior to and during these telephone contacts with CI-1, SELLER-1 was also in repeated telephone contact with DEVICE B. Several of these telephone contacts between SELLER-1 and DEVICE B were

mere seconds before or after telephone contacts between SELLER-1 and CI-1. UC-1 and CI-1 then met with SELLER-1 in the location indicated by SELLER-1. UC-1 provided SELLER-1 with government funds for the purchase of the methamphetamine. SELLER-1 indicated to UC-1 and CI-1 that they were meeting at this location because the source of the methamphetamine had wanted to meet there because it was closer to him. I know this location to be less than one mile from PHILLIPS' residence at 2824 N Marston Street, and to be significantly closer to 2824 N Marston Street than the aforementioned parking lot where SELLER-1 had met with UC-1 and CI-1 on multiple prior occasions.

14. On April 30, ATF personnel also conducted surveillance of John PHILLIPS. Approximately half an hour prior to UC-1 and CI-1 meeting with SELLER-1, ATF personnel observed John PHILLIPS exit a residence on the 1500 block of N Gratz Street, enter a black SUV, and drive away from the residence. PHILLIPS was not followed at this time. A short time later, ATF personnel observed PHILLIPS enter the front door of 2824 N Marston Street. Approximately 13 minutes later, ATF personnel observed PHILLIPS exit the front door of 2824 N Marston Street and walk to a black Chrysler SUV parked on the 2700 block of W Cambria Street. ATF personnel followed this Chrysler SUV as it drove from the 2700 block of W Cambria Street directly to the area of the location where SELLER-1, UC-1, and CI-1 were currently meeting. ATF personnel observed this Chrysler SUV arrive at this location and park immediately alongside SELLER-1's vehicle. ATF personnel observed SELLER-1 pick up and count the government funds that UC-1 had provided him minutes before, and then observed SELLER-1 enter the front passenger seat of this Chrysler SUV. ATF personnel observed as SELLER-1 briefly met with PHILLIPS in this Chrysler SUV. ATF personnel did not observe any other individuals in the Chrysler SUV besides PHILLIPS and SELLER-1. SELLER-1 then

exited this Chrysler SUV and walked to UC-1 and CI-1 with a black plastic bag in hand, which he provided to CI-1 and UC-1. This black plastic bag was found to contain approximately 114 grams of methamphetamine. Upon SELLER-1 exiting the Chrysler SUV, ATF personnel observed the Chrysler SUV immediately depart the location. Approximately half an hour later, ATF personnel observed this Chrysler SUV, now unoccupied, parked approximately half a block from 2824 N Marston Street.

15. The SELLER-1 pen register shows that SELLER-1 was in telephone contact with DEVICE B before and after an additional controlled purchase of methamphetamine on May 17, 2019. In summary, on May 16, 2019 CI-1 was in telephone contact with SELLER-1, during which CI-1 arranged to purchase methamphetamine from SELLER-1 on May 17, 2019. Later on May 16, 2019, the SELLER-1 pen register shows approximately six text messages were exchanged between SELLER-1 and DEVICE B. On May 17, 2019, CI-1 and UC-1 met with SELLER-1, who sold them approximately 222 grams of methamphetamine. During this meeting with SELLER-1 on May 17, 2019 and subsequent meetings with SELLER-1 on May 23, 2019 and May 31, 2019, SELLER-1 informed UC-1 and CI-1 that he wished to jointly purchase multiple pounds of methamphetamine with UC-1 and CI-1 in the near future, and to conduct additional such transactions on a monthly basis in the future. CI-1 and UC-1 agreed to conduct a joint purchase of multiple pounds of methamphetamine with SELLER-1 in the next several weeks. Approximately an hour after meeting with UC-1 and CI-1 on May 17, 2019, the SELLER-1 pen register shows that SELLER-1 received an incoming call from DEVICE B, which lasted for approximately two minutes and seventeen seconds. During these meetings between SELLER-1, UC-1, and CI-1 and during subsequent phone contacts between CI-1 and

SELLER-1, CI-1 and UC-1 arranged to conduct a transaction for multiple pounds of methamphetamine with SELLER-1 on the morning of June 11, 2019.

**June 11, 2019 Arrest of John PHILLIPS in the SUBJECT VEHICLE
and Search of 2824 N Marston St**

16. On June 7, 2019, the Honorable Timothy Rice, U.S. Magistrate Judge for the Eastern District of Pennsylvania signed a search and seizure warrant authorizing the search of 2824 N Marston Street. On the morning of June 11, 2019, law enforcement personnel established surveillance of 2824 N Marston Street, Philadelphia, PA. While there, they observed the aforementioned Audi SUV with Pennsylvania tag KXX-9805 parked a short distance from the residence. After a period of time, law enforcement personnel observed John PHILLIPS exit 2824 N Marston Street, walk directly to the Audi, and enter the driver's seat. At this time ATF personnel approached PHILLIPS, removed him from the driver's seat of the Audi, and arrested him. In a search of the Audi incident to arrest, ATF personnel recovered DEVICE A and DEVICE B, which were sitting on the driver's seat of the Audi where PHILLIPS had been seated. A short time later, law enforcement personnel executed the federal search warrant at 2824 N Marston St. Inside the residence, law enforcement recovered approximately 6 grams of alleged methamphetamine, a quantity of alleged crack cocaine, packaging consistent with narcotics distribution, a scale consistent with weighing and measuring narcotics for distribution, a loaded firearm magazine, and indicia for John PHILLIPS, among other items. Additionally, in the front bedroom of the residence, law enforcement recovered DEVICE C, along with several pieces of mail addressed to PHILLIPS and the aforementioned quantity of alleged crack cocaine. DEVICE C was seized by ATF pursuant to the search warrant for 2824 N Marston St. DEVICE A, DEVICE B, and DEVICE C were then transported back to the ATF offices at the U.S. Customs House, Philadelphia, PA. A short time later, I placed a call to 267-438-5835 (the DEVICE B

telephone number). Upon placing this call, I observed DEVICE B immediately begin to vibrate as though it were receiving an incoming call.

17. On June 11, 2019, the Honorable Richard Lloret, U.S. Magistrate Judge for the Eastern District of Pennsylvania, signed a criminal complaint and arrest warrant for PHILLIPS charging three counts of violating Title 21 United States Code, Section 841(a) - Distribution of over 50 grams of methamphetamine, and Title 18 United States Code, Section 2 - Aiding and Abetting of the same.

18. Based on my training and experience, and the training and experience of other agents, I know that individuals involved in drug trafficking, such as John PHILLIPS, often maintain more than one phone or more than one SIM card device in order to have multiple avenues to facilitate drug trafficking activities, in an attempt to avoid detection by law enforcement. I am aware that individuals involved in drug trafficking often use pre-paid cellular telephones, which do not maintain specific subscriber information, and/or phones subscribed to in the name of a third person in order to mask their direct linkage to telephones utilized in furtherance of drug trafficking activities. Further, those involved in drug trafficking often change SIM cards in order to make it difficult for law enforcement to determine their records. Based on my training and experience, as well as the training and experience of other agents, I know that individuals involved in drug trafficking also frequently switch telephone numbers and/or phones. Despite the constant switching of active telephone numbers, drug traffickers often keep old phones.

19. Based on my training and experience, I also know that drug traffickers commonly use their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their drug transactions. For example, I know that drug traffickers often store contacts lists,

address books, calendars, photographs, videos, audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

20. Specifically, I know that those involved in drug trafficking communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, I know that those involved in drug trafficking communicate with associates using cellular telephones and tablets to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

21. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. I am aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephones, are one of the few ways to verify the numbers (*i.e.*, telephones, pagers, etc.) being used by specific traffickers.

22. In addition, I know that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, *i.e.* photographs of accomplices and/or individuals common to co-conspirators. I

am also aware that drug traffickers often take photographs or make videos of drugs and drug proceeds with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

23. Furthermore, based on my training and experience and the training and experience of other agents, I know that drug traffickers often use a cellular phone's Internet browser for web browsing activity related to their drug trafficking activities. Specifically, drug traffickers may use an Internet search engine to explore where banks or mail delivery services are located, or may use the Internet to make reservations for drug-related travel. In addition, I know that drug traffickers also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with co-conspirators, and to display drugs and drug proceeds or to post photographs of locations where they have traveled in furtherance of their drug trafficking activities.

24. In addition, drug traffickers sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

25. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone

number assigned to each device, thus facilitating the identification of the phone as being used by an individual. In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

26. The Devices are currently in the lawful possession of the ATF. They came into the ATF's possession in the following way: DEVICE A and DEVICE B were seized during a search incident to arrest, and DEVICE C was seized during the execution of a search warrant. Therefore, while the ATF might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

27. The Devices are currently in storage at the ATF offices located at the U.S. Customs House, 200 Chestnut Street, Philadelphia, PA. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the ATF.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and

from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or

miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media

include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

29. Based on my training, experience, and research I know that the Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs, and allow them to connect to and access the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

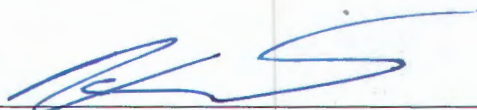
33. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

34. I submit that this affidavit supports probable cause for a search warrant

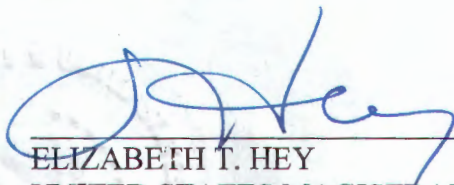
authorizing the search of the Devices described in Attachment A to seize the items described in Attachment B.

Respectfully submitted,



ROBERT WISE
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Subscribed and sworn to before me
on June 18, 2019:



ELIZABETH T. HEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is:

- a. Motorola, Model XT1921-3 smartphone, with IMEI: 354159100689047, hereinafter referred to as "Device A"
- b. LG, Model LM-X220MA smartphone, with IMEI: 352533-10-124096-2, hereinafter referred to as "Device B"
- c. ZTE, Model Z836BL smartphone, with IMEI: 862447032658403, hereinafter referred to as "Device C" (collectively referred to as "the Devices")

35. The Devices are currently located at the ATF offices located at the United States Customs House, 200 Chestnut Street, Philadelphia, Pennsylvania.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 21 United States Code 841(a) and Title 18 United States Code 2 involve John PHILLIPS, including:

- a. Electronic communications relating to the criminal activity,
- b. Telephone or address directory entries consisting of names, addresses, telephone numbers; logs of telephone numbers dialed, telephone numbers of incoming, outgoing or missed calls, text messages, schedule entries, stored memoranda, videos, social networking sites and digital photographs,
- c. Lists of customers and related identifying information,
- d. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions,
- e. Any information related to sources of controlled substances, including names, addresses phone numbers, and any other identifying information,
- f. Any information related to the methods of trafficking in controlled substances;
- g. Any information recording domestic and international schedule or travel related to the described criminal activity, including any information recording a nexus to airport facilities, airport security, or airlines,
- h. All bank records, checks, credit cards, credit card bills, account information, and other financial records,

- i. All data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system,
- j. Stored memoranda; stored text messages; stored electronic mail; stored photographs; stored audio; and stored video,
- k. Evidence of the times the device was used,
- l. Passwords, encryption keys, and other access devices that may be necessary to access any of the devices,
- m. Records of or information about Internet Protocol addresses used by the device,
- n. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "Favorite" web pages, search terms that the user entered into any Internet search engine, and records or user-typed web addresses, as well as evidence of the posting of videos, photos, or any material relevant to these crimes to any social networking site.
- o. Evidence of user attribution showing who used or owned the electronic devices at the time the things described above were created, edited, or deleted, such as logs phonebooks, saved usernames and passwords, documents, and browsing history.
- p. Any programs or applications that can aid in the aforementioned violations;

- q. Internet browsing activity and history, calendar entries, notes, memoranda, and digital documents, photographs and images, video and/or audio recordings
- r. any other information pertaining to the possession, receipt, and/or distribution of narcotics that were transmitted, stored, or received using items to be searched.
- s. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The “chip-off” method may be employed. Chip-off is an advanced digital data extraction and analysis technique which involves physically removing flash memory chip(s) from a subject device and then acquiring the raw data using specialized equipment. This process usually renders the cellular communication device unusable.